Les protocoles cryptographiques: comment sécuriser nos communications ?

Stéphanie Delaune

Chargée de recherche CNRS au LSV,

INRIA projet SecSI & ENS Cachan

21 Mars 2014

ENS Cachan

- 17 départements d'enseignement: mathématiques, informatique, chimie, génie mécanique, sciences sociales, ...
- 14 laboratoires de recherche:

Laboratoire Spécification & Vérification

L'enseignement à l'ENS Cachan

$\longrightarrow$ formation tournée vers les **fondements de l'informatique**

L'enseignement à l'ENS Cachan

$\longrightarrow$ formation tournée vers les **fondements de l'informatique**

- Les bases: calculabilité et logique, algorithmique, complexité, langages formels, programmation, ...
- Des enseignements plus poussés: preuves assistées par ordinateur, démonstration automatique, bioinformatique, ...

L'enseignement à l'ENS Cachan

$\longrightarrow$ formation tournée vers les **fondements de l'informatique**

- Les bases: calculabilité et logique, algorithmique, complexité, langages formels, programmation, ...
- Des enseignements plus poussés: preuves assistées par ordinateur, démonstration automatique, bioinformatique, ...

« La science informatique n'est pas plus la science des ordinateurs que l'astronomie n'est celle des téléscopes »

E. Dijkstra

La recherche au LSV

$\longrightarrow$ accroître notre confiance dans les logiciels critiques

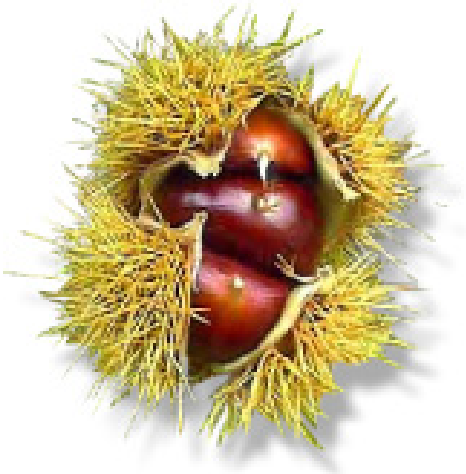
La recherche au LSV

$\longrightarrow$ accroître notre confiance dans les logiciels critiques

- logiciel: texte relativement long écrit dans un langage spécifique et qui sera exécuté par un ordinateur
- critique: une défaillance peut avoir des conséquences désastreuses en termes humains ou économiques

La recherche au LSV

Ennemi public numéro 1: le bug ...



... aussi connu sous le nom de bogue !

Dans la vie quotidienne !

Ariane V - 4 juin 1996

Un crash après 40 secondes de vol dû

...

Ariane V - 4 juin 1996

Un crash après 40 secondes de vol dû

...

à un bug logiciel !

1. 189 vols réussis pour Ariane IV,
2. réutilisation du logiciel de lancement d'Ariane IV,
3. ajout du nécessaire pour la nouvelle fusée.

$\longrightarrow$ Le logiciel d'Ariane IV contenait un bug !

Sonde Mars Climate Orbiter - 26 septembre 1999

Perte de la sonde due ...

Sonde Mars Climate Orbiter - 26 septembre 1999

Perte de la sonde due ... à un problème d'unité de mesure !

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
416500858395774644508840500943086599 9

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
416500858395774644508840500943086599 9

Affaire Serge Humpich (1997)

il factorise ce nombre de 96 chiffres et conçoit de fausses cartes bleues (les « YesCard »).

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
4165008583957746445088405009430865999

Affaire Serge Humpich (1997)

il factorise ce nombre de 96 chiffres et conçoit de fausses cartes bleues (les « YesCard »).

$\longrightarrow$ Depuis, le nombre utilisé pour sécuriser les cartes bancaires comportent 232 chiffres.

Comment assurer le bon fonctionnement de ces logiciels ?

Tests

- à la main ou génération automatique;
- vérification d'un nombre fini de cas.

Comment assurer le bon fonctionnement de ces logiciels ?

Tests

- à la main ou génération automatique;
- vérification d'un nombre fini de cas.

$\infty \infty \infty$ Accéder à l'infini: un rêve impossible ? $\infty \infty \infty$

Comment assurer le bon fonctionnement de ces logiciels ?

Tests

- à la main ou génération automatique;
- vérification d'un nombre fini de cas.

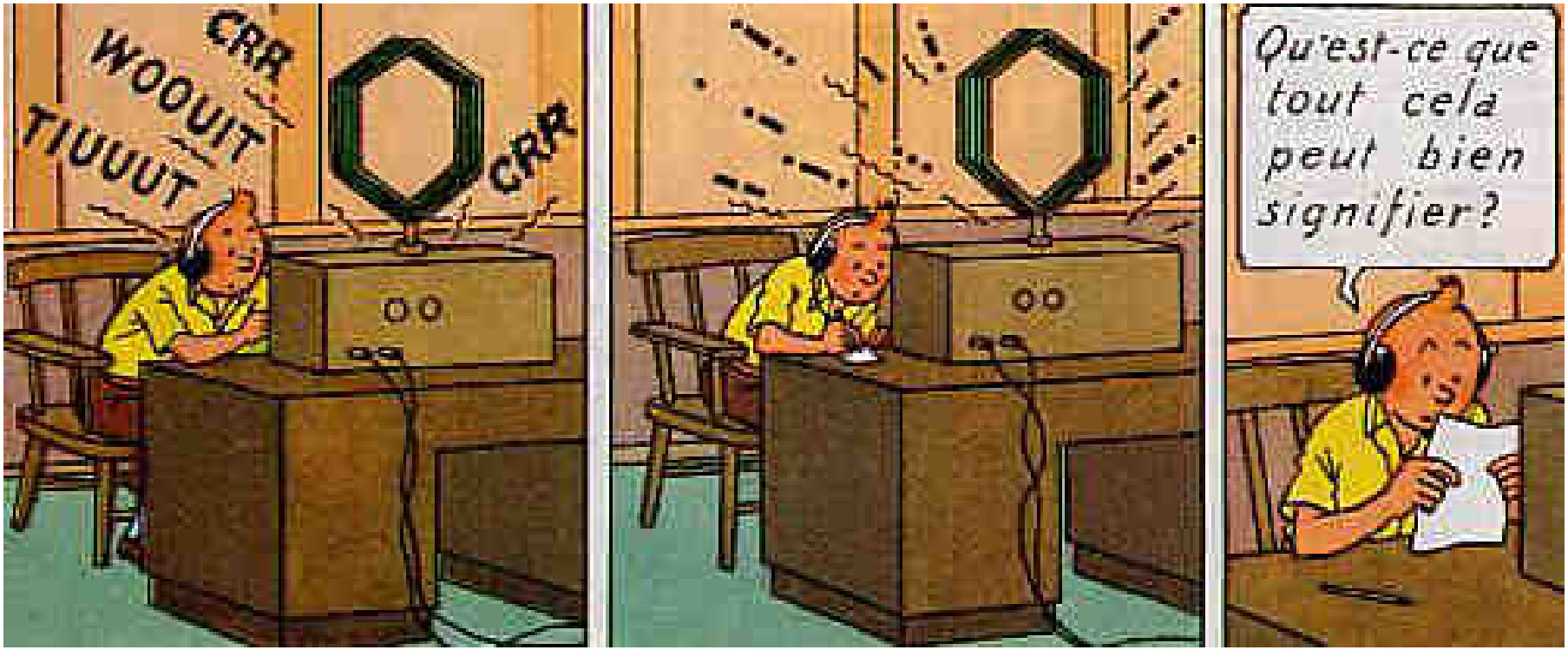
$\infty \infty \infty$ Accéder à l'infini: un rêve impossible ? $\infty \infty \infty$

Vérification (preuves formelles)

$\longrightarrow$ preuves mathématiques

- à la main ou à l'aide d'ordinateur;
- vérification de tous les cas possibles;
- plus difficile.

Les protocoles cryptographiques: comment sécuriser nos communications ?



Équipe projet SECSI

Sécurité des Systèmes d'Information

- 4 permanents: David Baelde, H. Comon-Lundh, S. Delaune, et J. Goubault-Larrecq.




- 1 ingénieur
- 3 doctorants

Protocoles cryptographiques

PayPal™

- petits programmes destinés à sécuriser nos communications (*e.g.* confidentialité, authentification)
- omniprésents dans notre vie quotidienne.

Protocoles cryptographiques

PayPal™

- petits programmes destinés à sécuriser nos communications (*e.g.* confidentialité, authentification)
- omniprésents dans notre vie quotidienne.

Protocoles cryptographiques

PayPal™

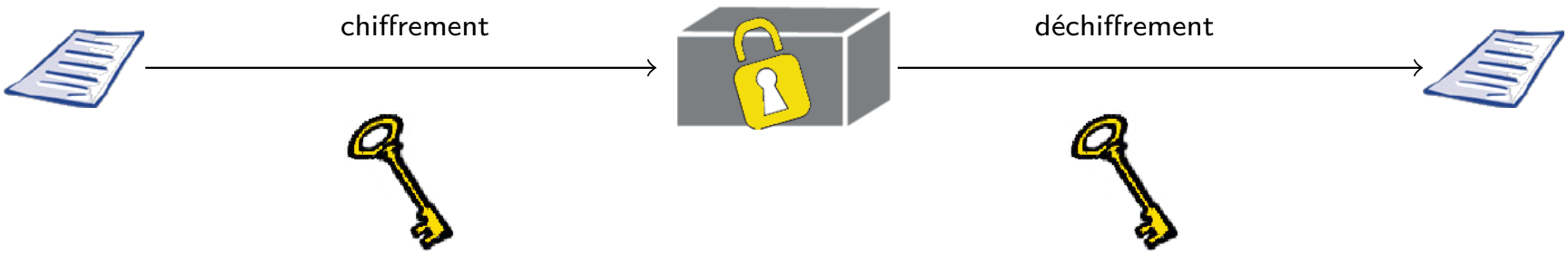
- petits programmes destinés à sécuriser nos communications (*e.g.* confidentialité, authentification)
- omniprésents dans notre vie quotidienne.

Nos informations personnelles sont en danger !

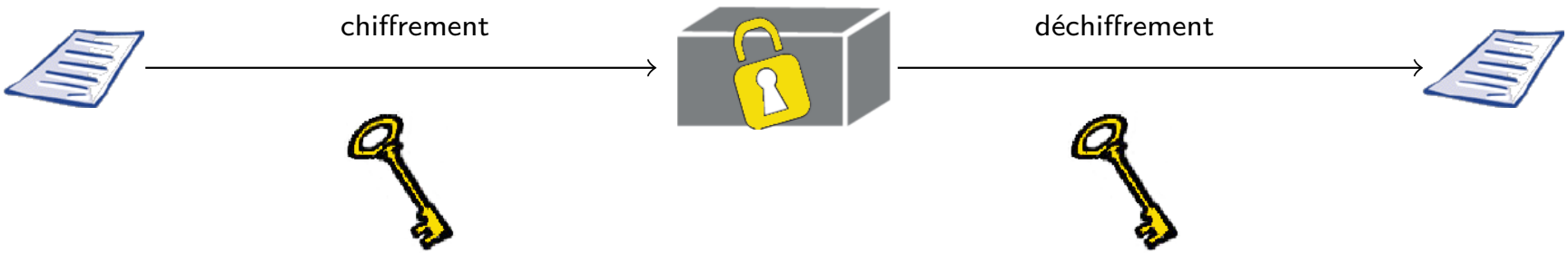
Le chiffrement

« VDYLJ QBVXU RUJH »

Chiffrement symétrique



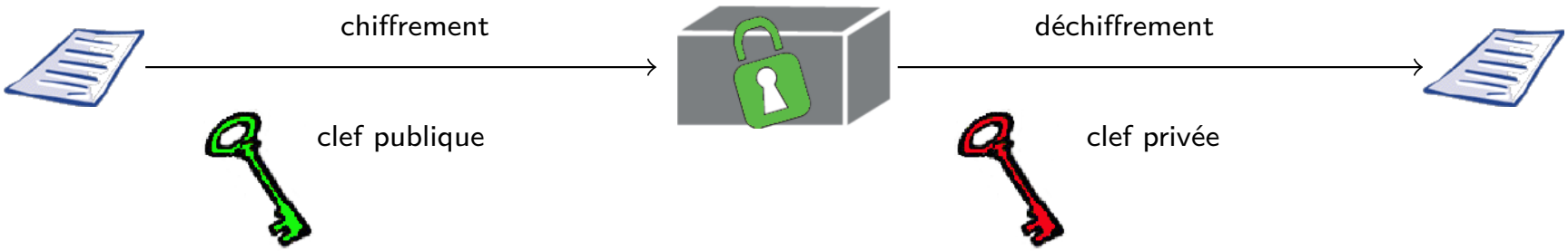
Chiffrement symétrique



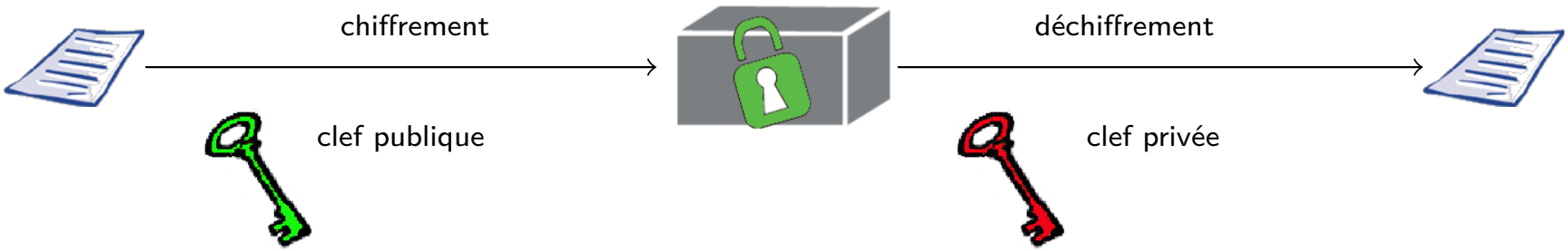
Quelques dates repères:

- 2000 avant J.-C.: traces de son utilisation par les Égyptiens
- 1920: machine Enigma
- 1977: Data Encryption Standard (DES)
- 2000: Advanced Encryption Standard (AES)

Chiffrement asymétrique (ou à clefs publiques)



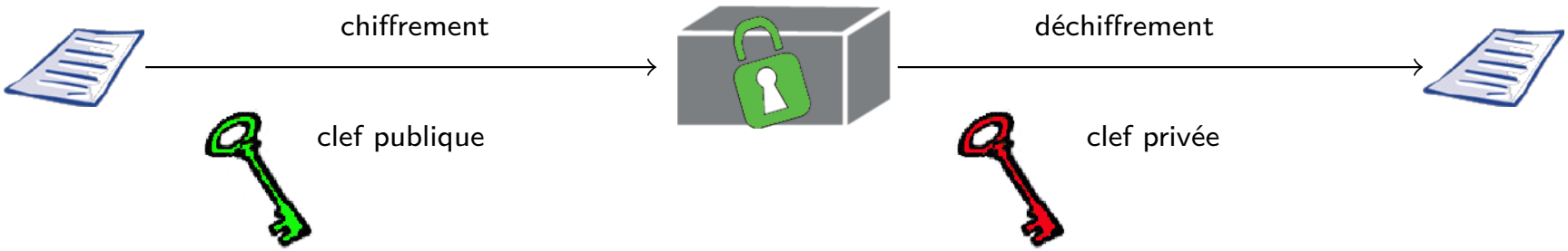
Chiffrement asymétrique (ou à clefs publiques)



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- cette méthode de chiffrement repose sur un problème mathématique bien connu: le problème de la factorisation.

Chiffrement asymétrique (ou à clefs publiques)



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- cette méthode de chiffrement repose sur un problème mathématique bien connu: le problème de la factorisation.

Tant que nous ne sommes pas capables de résoudre ce problème d'une façon efficace, la méthode de chiffrement RSA sera considérée sûre.

Mais chiffrer ne suffit pas toujours !

La carte bancaire

Le passeport électronique

Le vote électronique

Retour sur le protocole de carte bancaire

- Le client Cl insère sa carte C dans le terminal T.
- Le marchand saisit le montant M de la transaction.

- Le terminal vérifie qu'il s'agit d'une « vraie carte ».
- Le client entre son code.
  Si $M \geq$ €100, alors dans 20% des cas,
  - Le terminal contacte la banque B.
  - La banque donne (ou pas) son autorisation.

En détails (1/2)

4 acteurs: la Banque B , le Client Cl, la Carte C et le Terminal T

En détails (1/2)

4 acteurs: la Banque B , le Client Cl, la Carte C et le Terminal T

La **Banque possède**

- une clef privée – priv(B)
- une clef publique – pub(B)
- une clef symétrique secrète partagée avec la carte – K_{CB}

En détails (1/2)

4 acteurs: la Banque B , le Client Cl, la Carte C et le Terminal T

La **Banque possède**

- une clef privée – $\mathsf{priv}(B)$
- une clef publique – $\mathsf{pub}(B)$
- une clef symétrique secrète partagée avec la carte – K_{CB}

La **Carte** possède

- des données $Data$: nom du propriétaire, date d'expiration, ...
- la signature de ces données – $\{Data\}_{\mathsf{priv}(B)}$
- la clef K_{CB}, clef secrète partagée avec la banque.

En détails (1/2)

4 acteurs: la Banque B , le Client Cl, la Carte C et le Terminal T

La **Banque possède**

- une clef privée – $\mathrm{priv}(B)$
- une clef publique – $\mathrm{pub}(B)$
- une clef symétrique secrète partagée avec la carte – K_{CB}

La **Carte** possède

- des données $Data$: nom du propriétaire, date d'expiration, ...
- la signature de ces données – $\{Data\}_{\mathrm{priv}(B)}$
- la clef K_{CB}, clef secrète partagée avec la banque.

Le **Terminal possède**

- la clef publique de la banque – $\mathrm{pub}(B)$

En détails (2/2)

Le terminal T lit la carte C:

1. $C \rightarrow T : Data, \{Data\}_{\mathsf{priv}(B)}$

En détails (2/2)

Le terminal T lit la carte C:

1. $C \rightarrow T$: $Data, \{Data\}_{\mathsf{priv}(B)}$

Le terminal T demande le code:

2. $T \rightarrow CI$: $code?$
3. $CI \rightarrow C$: 1234
4. $C \rightarrow T$: code bon

En détails (2/2)

Le terminal T lit la carte C:

1. $C \rightarrow T$: $Data, \{Data\}_{priv(B)}$

Le terminal T demande le code:

2. $T \rightarrow CI$: *code?*
3. $CI \rightarrow C$: 1234
4. $C \rightarrow T$: code bon

Le terminal T demande l'autorisation à la banque B:

5. $T \rightarrow B$: *autorisation?*
6. $B \rightarrow T$: 45289
7. $T \rightarrow C$: 45289
8. $C \rightarrow T$: $\{45289\}_{K_{CB}}$
9. $T \rightarrow B$: $\{45289\}_{K_{CB}}$
10. $B \rightarrow T$: *ok*

Attaques sur la carte bleue

Initialement la sécurité été assurée par :

- cartes difficilement réplicables,
- secret des clefs et du protocole.

Attaques sur la carte bleue

Initialement la sécurité été assurée par :

- cartes difficilement réplicables,
- secret des clefs et du protocole.

Mais il y a des failles !

- le chiffrement n'est pas sûr (les clefs de 320 bits ne sont plus sûres);
- on peut faire des fausses cartes.

$\rightarrow$ "YesCard" fabriquées par Serge Humpich (1997).

La « YesCard »: Comment ca marche ?

Faille logique

$$
\begin{aligned}
1.C &\rightarrow T &&: \text{Data}, \{\text{Data}\}_{\text{priv}(B)} \\
2.T &\rightarrow CI &&: code? \\
3.CI &\rightarrow C &&: 1234 \\
4.C &\rightarrow T &&: ok
\end{aligned}
$$

La « YesCard »: Comment ca marche ?

Faille logique

$$
\begin{aligned}
1.C &\rightarrow T &&: \text{Data}, \{\text{Data}\}_{\text{priv}(B)} \\
2.T &\rightarrow CI &&: code? \\
3.CI &\rightarrow C' &&: 2345 \\
4.C' &\rightarrow T &&: ok
\end{aligned}
$$

La « YesCard »: Comment ca marche ?

Faille logique

$$
\begin{aligned}
1.C &\rightarrow T &&: \text{Data}, \{\text{Data}\}_{\text{priv}(B)} \\
2.T &\rightarrow CI &&: code? \\
3.CI &\rightarrow C' &&: 2345 \\
4.C' &\rightarrow T &&: ok
\end{aligned}
$$

Remarque : il y a toujours quelqu'un à débiter.
$\rightarrow$ ajout d'un faux chiffrement sur une fausse carte (Serge Humpich).

La « YesCard »: Comment ca marche ?

Faille logique

$$
\begin{aligned}
1.C &\rightarrow T &&: \text{Data}, \{\text{Data}\}_{\text{priv}(B)} \\
2.T &\rightarrow CI &&: code? \\
3.CI &\rightarrow C' &&: 2345 \\
4.C' &\rightarrow T &&: ok
\end{aligned}
$$

Remarque : il y a toujours quelqu'un à débiter.
$\rightarrow$ ajout d'un faux chiffrement sur une fausse carte (Serge Humpich).

$$
\begin{aligned}
1.C' &\rightarrow T &&: \text{XXX}, \{\text{XXX}\}_{\text{priv}(B)} \\
2.T &\rightarrow CI &&: code? \\
3.CI &\rightarrow C' &&: 0000 \\
4.C' &\rightarrow T &&: ok
\end{aligned}
$$

Le passeport électronique

Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

La puce RFID permet de stocker:

- les informations écrites sur le passeport,
- votre photo numérisée.

Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

La puce RFID permet de stocker:

- les informations écrites sur le passeport,
- votre photo numérisée.

Il est interrogeable à distance à l'insu de son propriétaire !

Passeport électronique 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

$\longrightarrow$ possibilité de récupérer la signature du porteur en interrogeant le passeport à distance

Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

$\longrightarrow$ possibilité de récupérer la signature du porteur en interrogeant le passeport à distance

"Faille" découverte sur les passeports belges

Passeport émis entre 2004 et 2006 en Belgique

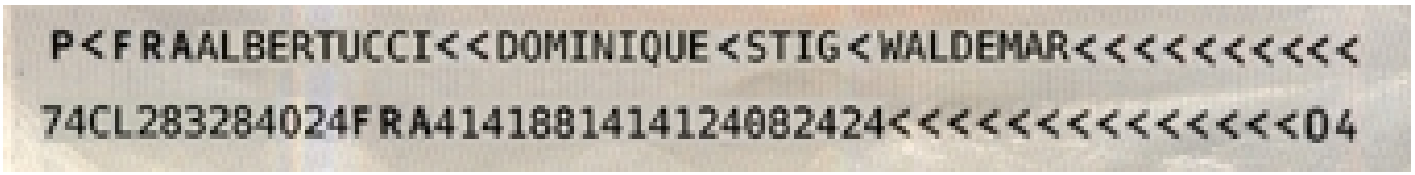
Passeport électronique — 2ème Génération

Passeport émis à partir de 2006 en France, en Belgique, . . .

Passeport électronique 2ème Génération

Passeport émis à partir de 2006 en France, en Belgique, . . .

$\longrightarrow$ mis en place d'un mécanisme (protocole BAC) qui permet de protéger nos informations personnelles



Avec ces deux lignes, on peut interroger la puce électronique.

Protocole BAC - objectif

Le Basic Access Control (BAC) protocole est un protocole d'établissement de clef qui doit assurer la protection de nos données personnelles ansi que la non traçabilité du passeport.

Protocole BAC - objectif

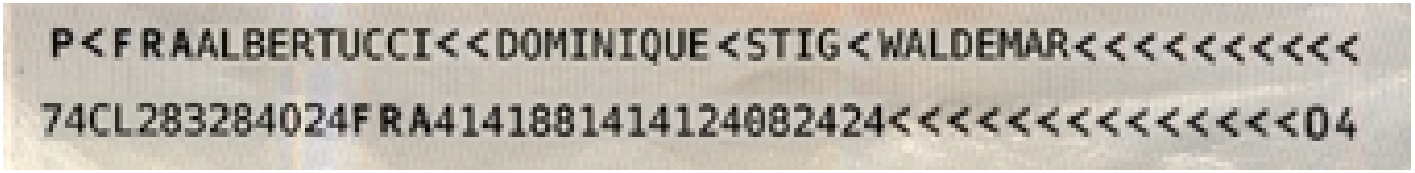
Le Basic Access Control (BAC) protocole est un protocole d'établissement de clef qui doit assurer la protection de nos données personnelles ansi que la non traçabilité du passeport.

ISO/IEC standard 15408

La non traçabilité a pour but d'assurer qu'un utilisateur peut utiliser plusieurs fois un service ou une ressource sans permettre à un tiers de faire un lien entre ces différentes utilisations.

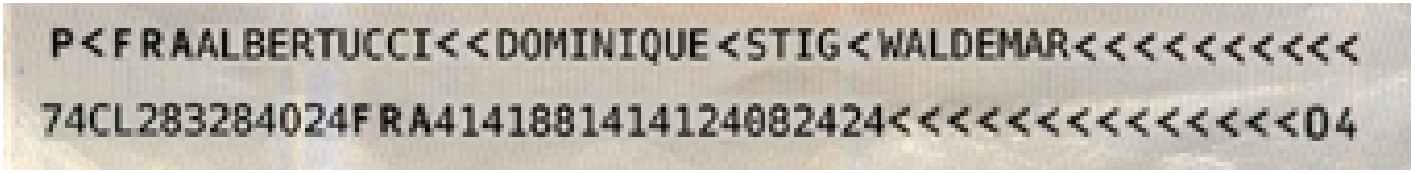
Protocole BAC - étape par étape

1. le lecteur dérive deux clefs K_E et K_M par lecture des lignes codées



Protocole BAC - étape par étape

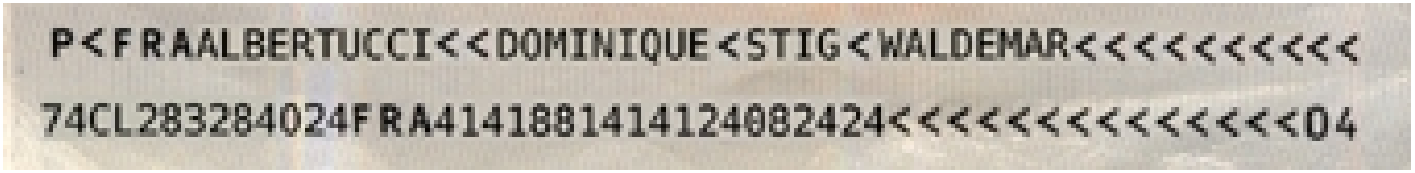
1. le lecteur dérive deux clefs K_E et K_M par lecture des lignes codées



2. Ensuite le passeport et le lecteur s'envoient des messages chiffrés pour établir une nouvelle clef K (utilisable qu'une seule fois);

Protocole BAC - étape par étape

1. le lecteur dérive deux clefs K_E et K_M par lecture des lignes codées



2. Ensuite le passeport et le lecteur s'envoient des messages chiffrés pour établir une nouvelle clef K (utilisable qu'une seule fois);

3. Ensuite, nos données confidentielles sont transmises chiffrées avec cette clef K.

Protocole BAC - version française

Dans la description du protocole:

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) mais ...
- ... ces messages d'erreurs ne sont pas précisés.

Protocole BAC - version française

Dans la description du protocole:

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) mais ...
- ... ces messages d'erreurs ne sont pas précisés.

Il en résulte une implémentation différente selon les nations, et ...

Protocole BAC - version française

Dans la description du protocole:

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) mais ...
- ... ces messages d'erreurs ne sont pas précisés.

Il en résulte une implémentation différente selon les nations, et ...

une attaque sur le passeport Français !!

Autres applications

Téléphonie mobile

- utilisation de pseudonymes temporaires pour assurer la non traçabilité

$\longrightarrow$ attaque similaire à celle trouvée dans le passeport électronique

Vote par Internet

- possibilité de voter de chez soi avec son ordinateur personnel

$\longrightarrow$ système le plus souvent **opaque** et **invérifiable** !!

Vote électronique

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

1936: une telle machine n'existe pas (Alan Turing)

... même dans le cas particulier des protocoles cryptographiques.

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Différentes pistes:

- résoudre le problème dans de nombreux cas intéressants,

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

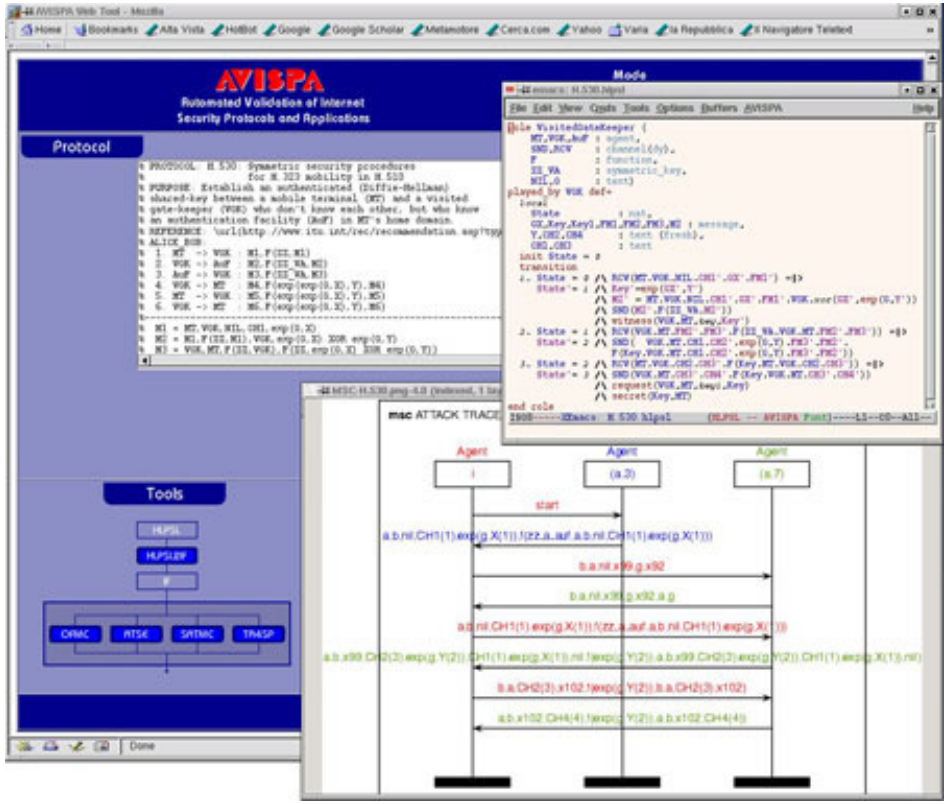
Différentes pistes:

- résoudre le problème dans de nombreux cas intéressants,
- proposer des procédures approchées,

  Exemple: si le vérificateur répond « oui » alors le logiciel est sûr, sinon on ne peut rien dire

Outil de vérification AVISPA

Outil disponible en ligne: `http://www.avispa-project.org/`



$\longrightarrow$ Projet Européen (France, Italie, Allemagne, Suisse)

Conclusion

Les méthodes formelles permettent une bonne analyse des protocoles cryptographiques.

- découverte de failles à l'aide d'outil de vérification;
- des preuves formelles de sécurité peuvent être obtenues automatiquement (sans intervention humaine).

Conclusion

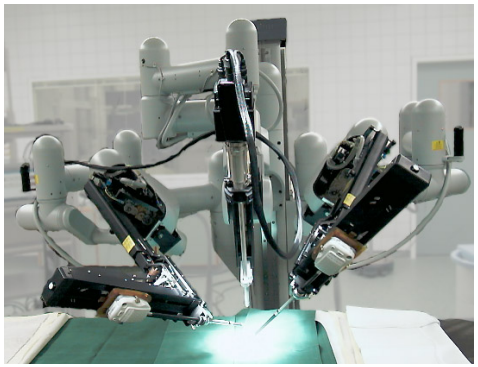
Les méthodes formelles permettent une bonne analyse des protocoles cryptographiques.

- découverte de failles à l'aide d'outil de vérification;
- des preuves formelles de sécurité peuvent être obtenues automatiquement (sans intervention humaine).

Il reste cependant beaucoup à faire:

- savoir analyser différentes propriétés de sécurité
  $\longrightarrow$ l'anonymat sous toutes ses formes!
- prendre en compte les propriétés mathématiques du chiffrement (e.g. chiffrement homomorphique), hachage, signature, ...
- réaliser ses analyses formelles dans des modèles plus réalistes.

Il reste beaucoup à faire (la suite)

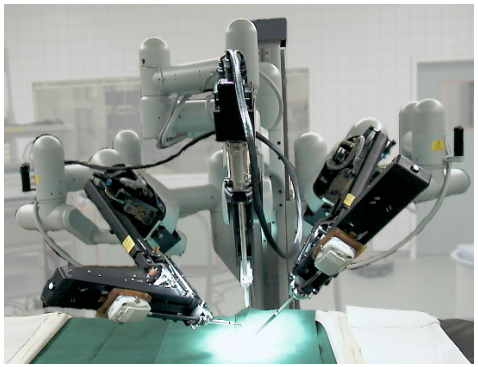


Les logiciels sont en perpétuelle évolution ...

- en vue de leur amélioration,
- pour développer de nouvelles applications
  $\longrightarrow$ vote électronique, robot en chirurgie, ...

... et sont de plus en plus complexes.

Il reste beaucoup à faire (la suite)



Les logiciels sont en perpétuelle évolution ...

- en vue de leur amélioration,
- pour développer de nouvelles applications
  $\longrightarrow$ vote électronique, robot en chirurgie, ...

... et sont de plus en plus complexes.

L'informatique est une **discipline** très vaste et en plein essor.

- informatique de la vérification,
- bioinformatique,
- exploration de données, ...